November 15, 2016
Version 1.0

Federal Cybersecurity Coding Structure

The Federal Government will begin using the new cybersecurity codes (i.e., the Cybersecurity Data Standard) contained in this document upon the Office of Personnel Management's (OPM's) issuance of implementation guidance on the new cybersecurity codes.

The new cybersecurity codes align to the November 2, 2016, version of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The new cybersecurity codes supersede the cybersecurity codes initially implemented by OPM in July 2013.

Agencies will assign these cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions.

Reference: The Federal Cybersecurity Workforce Assessment Act (Act), contained in the Consolidated Appropriations Act of 2016 (Public Law 114-113), was enacted on December 18, 2015 (see pages 735-737 at https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf). The Act requires the Federal Government to implement the NICE coding structure.

> *Federal Cybersecurity Workforce Assessment Act of 2015*
>
> > *Section 303. National Cybersecurity Workforce Measurement Initiative.*
> >
> > *(a) IN GENERAL.—The head of each Federal agency shall—*
> >
> > *(1) identify all positions within the agency that require the performance of information technology, cybersecurity or other cyber-related functions; and*
> >
> > *(2) assign the corresponding employment code under the National Initiative for Cybersecurity Education in accordance with subsection (b).*
> >
> > *(b) EMPLOYMENT CODES.—*

> *(1) PROCEDURES.—(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Director [of OPM], in coordination with the National Institute of Standards and Technology, shall develop a coding structure under the National Initiative for Cybersecurity Education.*

The **Employment Codes** called for in the Act are synonymous with the OPM cybersecurity codes assigned to each of the Work Roles in the November 2, 2016, version of the NICE Cybersecurity Workforce Framework (NICE Framework).

Contents

Cybersecurity Codes

In its 2013 and subsequent versions of the Guide to Data Standards (see pages A-103 – A-109 at http://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy-guidance/reporting-guidance/part-a-human-resources.pdf), OPM assigned a unique two-digit cybersecurity code to each of the categories and specialty areas in the NICE Framework version 1.0.

In 2016, the NICE Framework evolved to offer specific Work Roles expanding on the specialty areas in version 1.0. OPM has adopted a three-digit cybersecurity code for each of the Work Roles.

The NICE Framework organizes *information technology (IT), cybersecurity and cyber-related* work into seven high-level categories shown in Table 2; Table 3 provides descriptions of the specialty areas within each of the categories, as well as the original two-digit cybersecurity codes assigned to the specialty areas; and Table 1 shows the Work Roles, their new three-digit cybersecurity codes, and their relationship with specialty areas and categories.

NICE Cybersecurity Workforce Framework

The NICE Framework contains superset lists of tasks and knowledge, skills, and abilities (KSA) that are associated with cybersecurity work. Also in the NICE Framework, each Work Role is detailed showing the tasks and KSAs that fit within that Work Role.

It is intended that **ALL** *IT, cybersecurity and cyber-related* work is identifiable within the NICE Framework, and that work being performed by an *IT, cybersecurity or cyber-related* position is described by selecting one or more Work Roles from the NICE Framework relevant to that job or position and the mission or business processes being supported by that job or position. Alternatively, the Work Role(s) performed by an *IT, cybersecurity or cyber-related* position can be determined by first identifying in the NICE Framework the tasks carried out by the position and then selecting the Work Role(s) affiliated with those tasks.

Federal *IT, cybersecurity and cyber-related* positions may be comprised of more than one of the Work Roles described in the NICE Framework.

OPM Cybersecurity Codes Linked to the NICE Cybersecurity Workforce Framework

Table 1: Work Role Descriptions and New Cybersecurity Codes

Category	Specialty Area	Work Role	OPM Code	Work Role Description
Securely Provision	Risk Management	Authorizing Official/Designating Representative	611	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	612	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development	Software Developer	621	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	622	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture	Enterprise Architect	651	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	652	Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.
	Technology R&D	Research & Development Specialist	661	Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts

Category	Specialty Area	Work Role	OPM Code	Work Role Description
				comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning	Systems Requirements Planner	641	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation	System Testing and Evaluation Specialist	671	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development	Information Systems Security Developer	631	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	632	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain	Data Administration	Database Administrator	421	Administers databases and/or data management systems that allow for the storage, query, and utilization of data.
		Data Analyst	422	Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management	Knowledge Manager	431	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support	Technical Support Specialist	411	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).
	Network Services	Network Operations Specialist	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration	System Administrator	451	Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Systems Analysis	Systems Security Analyst	461	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor	731	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Compliance Manager	732	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer	711	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	712	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management	Information Systems Security Manager	722	Responsible for the cybersecurity of a program, organization, system, or enclave.
		COMSEC Manager	723	Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).
	Strategic Planning and Policy	Cyber Workforce Developer and Manager	751	Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
		Cyber Policy and Strategy Planner	752	Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.
	Executive Cyber Leadership	Executive Cyber Leadership	901	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Acquisition and Program/Project Management	Program Manager	801	Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.
		IT Project Manager	802	Directly manages information technology projects to provide a unique service or product.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
		Product Support Manager	803	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	804	Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.
		IT Program Auditor	805	Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst	511	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist	521	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response	Cyber Defense Incident Responder	531	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst	541	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze	Threat Analysis	Warning Analyst	141	Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.
	Exploitation Analysis	Exploitation Analyst	121	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis	All-Source Analyst	111	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and

Category	Specialty Area	Work Role	OPM Code	Work Role Description
				production requirements in support of planning and operations.
		Mission Assessment Specialist	112	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets	Target Developer	131	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
		Target Network Analyst	132	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.
	Language Analysis	Multi-Disciplined Language Analyst	151	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate	Collection Operations	All Source-Collection Manager	311	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors

Category	Specialty Area	Work Role	OPM Code	Work Role Description
				execution of tasked collection to ensure effective execution of the collection plan.
		All Source-Collection Requirements Manager	312	Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning	Cyber Intel Planner	331	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
		Cyber Ops Planner	332	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.
		Partner Integration Planner	333	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.
	Cyber Operations	Cyber Operator	321	Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.
Investigate	Cyber Investigation	Cyber Crime Investigator	221	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Digital Forensics	Forensics Analyst	211	Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	212	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Not Applicable	Not Applicable	Not Applicable	000	Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas.

Additional References

Table 2 – NICE Cybersecurity Workforce Framework Category Descriptions

Categories	Descriptions
Securely Provision	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Table 3 - NICE Cybersecurity Workforce Framework Specialty Area Descriptions with 2013 OPM Cybersecurity Codes

Categories	Specialty Areas	OPM Code	Specialty Area Descriptions
Securely Provision – 60	Risk Management	61	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
	Software Development	62	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
	Systems Architecture	65	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
	Technology R&D	66	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning	64	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
	Test and Evaluation	67	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
	Systems Development	63	Works on the development phases of the systems development life cycle.
Operate and Maintain - 40	Data Administration	42	Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Categories	Specialty Areas	OPM Code	Specialty Area Descriptions
	Knowledge Management	43	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support	41	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
	Network Services	44	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
	Systems Administration	45	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also, manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis	46	Conducts the integration/testing, operations, and maintenance of systems security.
Oversee and Govern - 70	Legal Advice and Advocacy	73	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
	Training, Education, and Awareness	71	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management	74	Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
	Strategic Planning and Policy	75	Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.

Categories	Specialty Areas	OPM Code	Specialty Area Descriptions
	Executive Cybersecurity Leadership	90	Supervises, manages, and/or leads work and workers performing cybersecurity work
	Acquisition and Program/Project Management	72/80	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life-cycle.
Protect and Defend - 50	Cybersecurity Defense Analysis	51	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
	Cybersecurity Defense Infrastructure Support	52	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response	53	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management	54	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
Analyze - 10	Threat Analysis	14	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Categories	Specialty Areas	OPM Code	Specialty Area Descriptions
	Exploitation Analysis	12	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis	11	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
	Targets	13	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis		Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.
Collect and Operate - 30	Collection Operations	31	Executes collection using appropriate strategies and within the priorities established through the collection management process.
	Cyber Operational Planning	33	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
	Cyber Operations	32	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate - 20	Cyber Investigation	22	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
	Digital Forensics	21	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.